

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
4 January 2001 (04.01.2001)

PCT

(10) International Publication Number
WO 01/01280 A2

(51) International Patent Classification⁷: **G06F 17/00**

(21) International Application Number: **PCT/US00/17858**

(22) International Filing Date: **28 June 2000 (28.06.2000)**

(25) Filing Language: **English**

(26) Publication Language: **English**

(30) Priority Data:
60/141,905 30 June 1999 (30.06.1999) US
09/451,469 30 November 1999 (30.11.1999) US

(71) Applicant (for all designated States except US): **CATALOG CITY, INC.** [US/US]; 510 Lighthouse Avenue, Pacific Grove, CA 93950 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **LORENZEN, Lee,**

J. [US/US]; 619 Spazier Avenue, Pacific Grove, CA 93950 (US). **ZIMMERMAN, Jordan** [US/US]; 10 Victoria Vale, Monterey, CA 93940 (US).

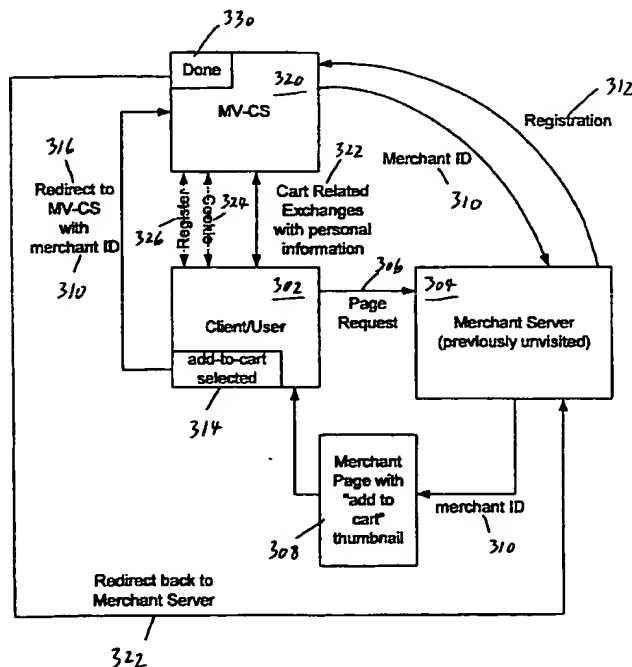
(74) Agent: **WHEELER, Jeffrey, D.**; Beyer Weaver & Thomas, LLP, Post Office Box 130, Mountain View, CA 94042-0130 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: **METHOD AND SYSTEM FOR SHARING COOKIE INFORMATION DURING INTERNET TRANSACTIONS**



(57) Abstract: A method and system architecture that provides for sharing of cookie information between different web server devices. A central server communicates with a merchant server and a client device. The merchant and client register with the central server and are assigned respective identifiers (IDs). In one embodiment, a client contacts a merchant server and is presented with an option to invoke an e-commerce operation. The e-commerce operation directs the client to the central server with the merchant ID, and the client cookies

[Continued on next page]



patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *Without international search report and to be republished upon receipt of that report.*

are transferred with the interaction. The central server uses the merchant ID and cookie information to retrieve information. The client thereafter receives certain pages from the central server, as customized with the retrieved information, so that the client experience is personalized. The pages may even be made to appear that they originated from the merchant server. In another embodiment, a client contacts a merchant server and is re-directed to the central server with the merchant ID. The central server retrieves information via the merchant ID and client cookie. The client is re-directed back to the merchant server with identifier information passed as an address parameter. The merchant server then uses this identifier information to serve a customized/personalized page to the client.

METHOD AND SYSTEM FOR SHARING COOKIE
INFORMATION DURING INTERNET TRANSACTIONS

REFERENCE TO PRIOR RELATED APPLICATIONS

This application claims priority of U.S. provisional patent application No. 60/141905, filed June 30, 1999, entitled "Multi-Vendor Internet Commerce System For E-Commerce Applications And Methods Therefor," Attorney Docket No. CCTYP001P, which is hereby incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to a method and system architecture for sharing cookie file information between multiple Internet transactions. More specifically, the present invention provides for recognition of a user by a web site (or domain) that has not previously been visited by a user.

BACKGROUND OF THE INVENTION

The Internet is a worldwide system of computer networks -- or a network of networks -- wherein users at any one computer can, if they have permission, get information from any other computer. The Internet was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANet. The original aim was to create a network that would allow users of a research computer at one university to be able to "talk to" research computers at other universities. A side benefit of ARPANet's design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster.

Today, the Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in private networks referred to as intranets and extranets. Each interacting computer has a copy of TCP/IP (via the browser or

the like). TCP/IP is a two-layered program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such a Web page) by another computer (a server) in the network. An example of an early prior art e-commerce site might use individualized session links in order to deal with different customers. An IP link is established for each contacting machine, and no other information is requested from a user. These sessions provide no way of identifying a particular user because no identifying information has been asked for, or provided. The intent of such systems was to prevent any barriers to commerce being carried out across multiple sites. When each link was terminated, however, no information about the user was retained for later reference.

A cookie is a special text file that a Web site places on a user's hard disk so that the Web site can remember something about the user at a later time. In particular, client-side variables are provided with user information and/or instructions which cause (as a function of Hypertext Markup Language, HTML) the cookie file to be set with that particular information.

Typically, a cookie records a user's identity or preferences when using a particular site. Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent of all other requests. For this reason, the Web page server would have no memory of the pages, or other information, which might have been sent to a user during a previous visit. A cookie is a mechanism that allows the Web server to store its own particularized file about a user on the user's own computer. The file is typically stored in a subdirectory of the browser directory (for example, as a subdirectory under the Netscape directory). The cookie subdirectory will contain a cookie file (or files) for each Web site visited by a user, provided that Web site uses cookies.

The Internet is facilitating ever-expanding commerce opportunities for individuals and companies to sell goods and services to customers through a web site. Since these opportunities are oriented towards customer service, it becomes important to provide as much individualized customer attention as possible. Business experts (i.e. Dale Carnegie and the

like) have continually stressed the power of referring to a potential customer by their name in order to secure trust and friendship from that customer. To facilitate such individualized contact, new users are often asked to register at each new web site they contact. This is problematic in that the registration process is often lengthy and cumbersome. This registration process can result in the setting of many different cookies through HTML (Hypertext Markup Language) commands returned from the web site through the user's browser. If the user then contacts that web site again (from the machine where the cookies are stored), the cookies will be sent to the web site with the user's request for a web page. The web site will thereby have information pertaining to that individual user. Individualized greetings, screens, and the like, can be provided to the user based upon such information. New users, however, will either be greeted generically, or they must endure the aforementioned registration process over and over again for each new web site visited.

Another problem exists when a user chooses to contact a web site from a different browser or machine than was originally used. The cookie files are stored on the hard-disk of the machine originally used to contact the web site. The cookie files are also associated with a particular browser. If the user travels to a different machine (or uses a different browser on the same machine), none of the cookies that have previously been set will be available. If the user has visited the site before, then the web site might offer the user a truncated form of the registration process, wherein a user identification and password are entered. From these data entries by the user, the web site will be able to re-identify the user and set the appropriate cookies on the particular machine (or browser) being used.

Still another problem is that a particular cookie file can only be accessed by the web server (or domain name) which established the cookie file. For valid security reasons, the Internet will generally preclude the sharing of data across multiple domain names. This prevents different web sites from intercepting or sharing information about the different users whom are contacting the sites. Hence, if a user has endured the lengthy registration process at one web site, and has a cookie file relating to such registration information, that cookie information still cannot be used by other web sites. In practice, the browser will only send back cookies to a particular web site which has been created by that web site.

Accordingly, what is needed in the field is a method and system that provides for sharing of cookie file information between multiple Internet transactions (or machines). More

specifically, the solution should at least provide the illusion and/or convenience (from a user standpoint) that such user information has been made available to many different sites, but without sacrificing security issues. The solution should provide for recognition of a user by a web site (or domain name) that has not previously been visited by a user. The process should be virtually invisible to the user, and yet should provide any participating web sites convenient access to such shared information services.

SUMMARY OF THE INVENTION

To achieve the foregoing, and in accordance with the purpose of the present invention, a method and system architecture are disclosed that allows cookie information to be shared between multiple web sites. In one embodiment, a client/user contacts a new merchant server, and is directed back to a central server wherein certain client-identifying cookie information can be retrieved and used by the central server. In another embodiment, the client contacts a new merchant and is re-directed back to a central server that retrieves information from the client's cookie file. The client is re-directed back to the merchant site with certain identification information passed back in a parameter associated with the URL.

According to one embodiment, the present invention takes advantage of the fact that certain information is known about a client/user on a centralized site or server. The client/user will have previously registered with the central server -- either by directly contacting the central server, or as a function of other shopping experiences (or contacts) with a merchant server which is registered with the central server. The registered merchant will be assigned an identifier (ID, token, or the like) which can be used to access various information about the merchant. This information might include the merchant's name, color schemes, logos, or any other elements relating to an interface presentation style that the merchant would prefer to be used when dealing with a client/user. Such information can be stored in a database (or the like) associated with the central server.

The client/user contacts a merchant web site that has not previously been contacted by that client/user. As such, no cookies can be transferred from the client/user to the merchant site. The merchant site then directs or links the client/user back to the central server, with the merchant ID being passed along in the process. The client/user thereafter interacts directly

with the central server (instead of the merchant server). Cookie information will be transferred between the client/user and the central server. The merchant ID also allows the central server to pull up certain interface presentation style information pertaining to the merchant. Web pages are thereafter provided to the client/user from the central server, these pages having a certain look/feel of the merchant. The directing of the client/user to the central server is substantially invisible to the client/user, and yet provides a more personalized exchange of information via the client/merchant information stored in (or with) the central server.

Hence, with this embodiment, the invention is able to present a page that looks as if the client/user is still interacting with the original merchant site. The URL or domain name on the browser address line will read something different than was originally entered, but the client/user typically does not pay much attention to what happens on the URL address line.

The cookies -- which might exist for the client/user (or be prompted for creation) -- can be accessed by the central server, and can thereby be utilized to enhance the client/user's interactive experience. In this manner, the present invention is able to share information across domain names, when in essence only one source of such information exists (e.g. the central server). The information is presented in a different manner so that the client/user is generally unaware that the system has moved the client/user to a different domain in order to get around the limitation that cookies cannot be shared between domains. By virtue of coming to a single domain, if a user has previously visited another central server merchant site, then certain client/user information will be readily available.

Any of a variety of e-commerce (or other such) operations might be used to invoke direction back to the central server from the merchant site. An example application would include an electronic shopping cart, wherein the client/user visits a new merchant site, selects an item for purchase, and then clicks-on an "add-to-cart" button. Further shopping cart interactions (i.e. view cart, modify contents, etc.) will be between the client/user and the central server. The shopping cart can be presented to the client/user with items selected from this merchant site, along with all other items from other central server registered merchants. Upon completion of shopping cart interactions, the client/user can be routed/linked back to the merchant server for further shopping on that merchant site, or for linking to other sites.

Still another embodiment of the present invention allows for client/user to contact a new merchant web site, and be greeted with a personalized message or the like. This is achieved by

re-directing the client/user back to a central server, wherein client information is retrieved from cookie files that are accessible by the central server. The central server re-directs the client/user back to the merchant web site, and passes along user information (i.e. the user name). The merchant web site then uses this information to pass a personalized greeting back to the client/user.

According to one configuration, at least one merchant web site will have registered with a central server, thereby creating a merchant ID. Certain merchant-side software can also be supplied via the central server for detecting a triggering event for the various re-directions described herein. The client/user will request a page from this merchant web site via the standard mode of typing a URL into the address line of a browser. One triggering event might be a lack of parameters in the URL request. If identification is needed, the client/user will be re-directed back to a central server, with the re-direction carrying the merchant ID information, in an address parameter or the like. The client/user then requests information from the central server and cookie file information is transferred, if available. Otherwise, the client/user might be prompted to register with the central server and the cookie will be set. The client/user identity can be retrieved via the cookie information and the client/user is thereafter re-directed back to the merchant server with this identification information attached as an address parameter. The merchant server utilizes this information to return the originally requested page information, along with a personalized greeting or the like, as derived from the identification information.

These and other advantages of the present invention will become apparent upon reading the following detailed descriptions and studying the various figures of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further advantages thereof, may best be understood by reference to the following description taken in conjunction with the accompanying drawings in which:

Figure 1 illustrates a prior art block diagram of a client/user contacting a web site for the first time and being directed to register.

Figure 2 illustrates a prior art block diagram of a client/user contacting a web site that has already been visited.

Figure 3 illustrates, according to one aspect of the present invention, a block diagram of a system for re-directing a client/user back to a Multi-Vendor Central System (MV-CS) so that
5 accessible merchant and client/user data can be retrieved and used.

Figure 4A illustrates, according to another aspect of the present invention, a block diagram of a client/user request being re-directed multiple times in order to provide client-specific information back to the client in the context of a page request.

Figure 4B illustrates, according to still another aspect of the present invention, a block
10 diagram of a client/user request being re-directed multiple times, but the client is not recognized and is re-directed to register with the central server.

Figure 5 illustrates, according to another aspect of the present invention, a flow chart of certain representative steps used to set a cookie and utilize the cookie information.

Figure 6 illustrates, according to another aspect of the present invention, a flow chart of
15 certain representative steps used to return cookie setting code to the user's browser.

Figure 7A illustrates, according to one aspect of the present invention, a generalized computer configuration for use with the present invention.

Figure 7B illustrates, according to one aspect of the present invention, a generalized computer configuration for use with the present invention.

20

DETAILED DESCRIPTION OF THE INVENTION

An invention is described herein relating to a method and system architecture that provides for sharing of cookie file information between different web sites or domains. In the following description, numerous specific details are set forth in order to provide a thorough
25 understanding of the present invention. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without some or all of these specific details. In

other instances, well-known structures and/or process steps have not been described in complete detail so that the present invention is not obscured in an unnecessary manner.

For ease of discussion, the following detailed description is made with reference to a client/user, a merchant server, and a central server (or multi-vendor central system, MV-CS), all of which interact with each other over network connections, such as the Internet. These example elements are provided for ease of discussion and are not meant to be limiting in any way. The invention provides, regardless of the devices or media used, various embodiments for the sharing of cookie information between web domains. This sharing is facilitated by the central server (or MV-CS) which is able to access (or establish) cookie file information from the client/user machine. The central server can provide interaction with the client/user, or re-direction back to the merchant server, while utilizing such cookie information to provide a personalized user experience.

The incorporated reference entitled "Multi-Vendor Internet Commerce System For E-Commerce Applications And Methods Therefor" provides examples of central server systems. It should be noted that the present invention is not intended to be limited to such specific embodiments. The central server might include any server and/or computing device configured to provide the functions, and/or facilitate the processes or methods described herein.

In accordance with one aspect of the present invention, a client/user contacts a new merchant server, and is directed to a central server for interaction pertaining to a selected operation. The merchant server is registered with the central server, and various merchant information is available thereon. The client/user might also be registered with the central server, and cookie information can flow between the client/user machine and the central server machine. Such client-identifying cookie information can be retrieved and used by the central server, along with the merchant information, to present customized and/or personalized web pages to the client/user. The client/user is then experiencing a set of customized pages, but is generally unaware that they have been interacting with the central server, and not the merchant server. Upon completion of the selected operation, the client/user is directed back to the merchant server and beyond.

According to still another aspect of the present invention, the client contacts a new merchant. The merchant server includes merchant-side software that triggers on a certain event, such as the lack of (or additional) parameters sent in the client/user's request to the merchant server. The client/user is re-directed back to a central server that retrieves
5 information from the client's cookie file. The central server thereafter re-directs the client/user back to the merchant site with certain identification information passed back in a parameter associated with the page request. The merchant site uses this identification information to supply a customized page to the client/user, which might provide a personalized greeting or the like.

Referring now to Figure 1, a prior art block diagram 100 is shown which illustrates the exchange of cookie information between sites. A client (or user) 102 is shown sending a page request 104 to a web server 106. The client 102 would typically be using a web browser (e.g. Navigator or Explorer) to send a page request to a web site or domain name on the Internet. In this example, the web server has been previously unvisited by this client. As a result, no
15 cookie files (or related information) exist on the client computer 102. The page request 104 is sent without such cookie information, and this prompts the web server 106 to prompt the user to register on the site. After any variety of information and screen exchanges, the registration information 108 is stored on a database 110 associated with the web server 106. The database might store the information -- in any format -- for direct retrieval in its original form.
20 Typically, however, the data will be tabulated and assigned an identification or mapping index for retrieving the information. This identification (ID) will be returned to the web server 106. The ID (or other such recognizable item) can thereafter be incorporated into cookie information for storage on the client device 102. A page response 114 is returned back to the client with instructions for setting this cookie information in the appropriate file on the client
25 machine.

Referring now to Figure 2, yet another prior art block diagram 200 is shown, wherein a subsequent page request is sent from the client to the web server which has previously been visited. The client (or user) 202 is shown sending a page request 204 which also sends all the available cookie files on the client machine 202 over to the web server 206. These cookie files
30 will generally be available, since this client has previously visited the web site. The cookie might contain any of a variety of information. Their might also be multiple cookies (and/or

cookie files) associated with this web site. Cookies are set via strings of HTML commands in a file, wherein the file might (in turn) refer to other files. These strings are not usually related to what a user views on the screen, but instead serve to instruct the browser regarding various browser tasks -- like setting particular cookies. To convey a large amount of information, however, multiple cookies are not necessary and might even be considered a waste of bandwidth. Instead, a user ID 208 can be contained within the cookie information. The user ID 208 is used to access the database 210, which is generally associated with the web server 206. The ID 208 results in the return of user information 212 back to the web server 206. Now that the user has been identified, the page response 214 might provide a customized page based upon the now known user information (e.g. "Welcome identified client"). Further interactions by this client with this web site will also have available the cookie file to provide such information.

Certain detriments (or limitations) of the aforementioned configurations include, but are not limited to, the following: 1) Inherent to HTML, the client machine will only provide cookies (if they exist) to the same web server (or domain server) that was associated with creating those cookies. In working around this limitation, a user is generally not able to leverage the fact that they might be registered at other sites. 2) A person needs to register at each new site that is visited. Therefore, many different cookies are being created and stored on the user's computer. A wealth of user registration information might exist in any of a variety of different cookie files, but such information would not generally be available to multiple sites. 3) A client might use the same machine to contact a web site, but if the browser is different from the one setting the cookies, then that browser cannot access those cookies. The user would be prompted to endure the full process of re-registering with the web site. Alternatively, a truncated form of registration might be used, wherein the user would be required to "log in" via entry of an identification and password. 4) Inherent security precautions have been designed into existing Internet protocols (e.g. HTTP and HTML) to prevent trading of information between different web servers. The security measures advantageously prevent "unknown" web servers from retrieving information for a user's computer (via cookies or otherwise). Such security measures are important to preserve; yet it would also be beneficial to share information between multiple servers.

Referring now to Figure 3, a block diagram 300 is shown of one embodiment of the present invention, wherein a certain representative e-commerce operation directs a client 302 to interact with a central server 320. The central server might be a computer configured to handle requests for certain information regarding a multitude of vendors. While not intended to be limited to any specific embodiment, the Multi-Vendor Central System (MV-CS), and similarly the Multi-Vendor Internet Commerce System (MV-ICS) -- as described in the priority application -- are examples of such. The central server thereafter provides personalized interaction with the client via client cookie information, and merchant identification information, which has been passed to the central server.

As shown in Figure 3, a client/user 302 sends a page request 306 to a merchant server 304. In this instance, the merchant server has never been visited by the client/user. As a result, there is no cookie information to be passed from the client 302 to the merchant server 304. The merchant server 304 returns the requested page 308, which also includes an "add-to-cart" click-through area (i.e. a link, or a thumbnail) on the page. Also passed with this page of information 308 is a merchant identifier (ID) 310. The merchant ID was previously established via the merchant server 304 going through a registration process 312 with the central server 320. The merchant ID 310 is thereafter established and returned to the merchant server 304. The merchant ID 310 might consist of an index into the databased merchant-related information. The ID 310 can include multiple pieces of information such as a syndication item, and/or a CCP ID or the like, to identify the merchant. Anytime a private identifier is being passed from one device to another, the result will likely be encrypted. Receiving devices would then be able to use a token or key to decrypt the ID, as required.

The registration process 312 can also allow the merchant to provide the MV-CS 320 with certain information which might be particular to the merchant, such as color schemes, company emblems, or the like. Collectively, such information might be referred to as an interface presentation style for that merchant. This information will be used by the MV-CS to display pages to the user so that they appear as if they have been presented directly by the merchant server.

The client/user 302 will continue to interact with the merchant server 304, until a certain e-commerce operation is invoked (via a click-through, or the like). In this instance, the click-through includes an "add-to-cart" operation 314. During an add-to-cart operation, an item that

the client has selected will be added to the client's electronic shopping cart for display, and later check-out operations. The selection of this add-to-cart operation serves to re-direct the client/user 302 to the MV-CS 320 via the link 316. While referred to as a "re-direction," the link 316 is actually a "direction" or a hyperlink to MV-CS 320 with certain parameters being passed. For instance, the merchant ID (310) will be passed to the MV-CS 320 with this direction. The client will then interact with the MV-CS 320, rather than the merchant server 304.

The "selection operation," which routes the client/user to the MV-CS, is not intended to be limited to the example "add-to-cart" operation. Virtually any operation wherein it is desired to maintain centralized information concerning a particular client/user would benefit from the principles taught in this invention. By re-directing the client/user to the MV-CS, the system can take optimum advantage of the situation where the merchant has registered with the central server, and the client/user has registered with the central server, but the client/user has not previously contacted the merchant server. The merchant server knows nothing about this client/user. However, the MV-CS knows about this client/user and the re-direction operation facilitates providing an individualized customer experience based upon such known user information. Other example selection operations might include (but are not limited to): "Add to wish list" wherein a user adds a product that he/she wishes to receive as a gift to a list which is accessible by other people; "Add to gift registry" wherein a user adds a product to a gift registry which is accessible by other people; "View shopping cart" wherein the user views the collection of items placed in the shopping cart, even if from different merchant sites; "View account" wherein the user can view the status of their account (e.g. billing, payment, etc.); "View my order history" wherein the user can view when orders are placed, or the status of such orders; and "Address book" wherein the user can retrieve/edit/modify addresses, or the like.

If the client/user 302 has previously registered with the central server 320, then a cookie file (or files) will exist for this user, the cookie files being accessible by the central server 320. These cookie files 324 will be sent to the MV-CS 320 when the client/user 302 sends a page request. Accordingly, the central server 320 will be able to identify certain information about the user, whereas the merchant server would not be able to receive these cookie files. The MV-CS 320 can then compile the user information, along with certain merchant information

(e.g. color scheme, etc.) as retrieved from a database or the like associated with the MV-CS, via the merchant ID 310. Element 322 shows cart related exchanges between the client/user 302 and the MV-CS 320. These exchanges might consist of customized web pages that are conveyed to the client/user. The pages can contain, for instance, personal information (e.g. "John Doe's shopping cart") and/or merchant information (e.g. color scheme, merchant identifiers, etc.).

As such, the client/user 302 can be presented with the illusion that the merchant server device 304 is presenting the various web pages. If the "look and feel" of the pages reflect those of the merchant server, than the client/user is generally unaware of the actual source of the web page. On the client/user side, the Uniform Resource Locator (URL) line on the browser is the most obvious indication of the actual source of the web page. This line will change to reflect the direction (or link) to the MV-CS device. However, most users will remain unaware and/or unconcerned as to the source of the pages, even when this URL line changes.

The client/user 302 might not be registered with the MV-CS 320. As a result, a cookie file will not exist for this client. A registration process 326 can be invoked, wherein the client/user will be prompted for various information. The user information can be databased, with a corresponding user ID (e.g. map index or the like) assigned to the client/user. This user ID can thereafter be set in the cookie file 324, which resides on the client/user machine 302. Subsequent exchanges between the MV-CS 320 and the client/user 302 will retrieve the user information via the user ID derived from the cookie file.

Upon completion of the selected operation (as figuratively shown by the "done" box 330), the client/user 302 will be re-directed back to the merchant server 304, via the link shown as 332. The client/user 302 can thereafter proceed with other transactions with the merchant server 304, or move onto other merchant sites via newly entered links to the those sites.

In the aforementioned diagram, a configuration is provided wherein the client/user invokes a certain operation and is linked back to the central server. The client/user then interacts with the client/user to receive pages and information with the merchant interface presentation styles. It would also be useful if the client/user could interact directly with the

merchant server -- with the merchant server being able to greet, or interact with, the user in some personalized manner -- even if the client/user has not previously contacted the merchant server. This would involve retrieving and sending some form of personal information to the merchant server, but without (significantly) interfering with the client session.

5 Referring now to Figure 4A, a block diagram 400 is shown of a configuration for providing such interaction with the client/user. A client/user 402 is shown sending a page request 404 to the merchant server 406. In one instance, no cookie files will be sent because the client/user 402 has not previously contacted the merchant server 406. If, on the other hand, the merchant server 406 has been previously contacted by this client/user 402, then those
10 cookies associated with the merchant server 406 will be sent with the page request 404.

The merchant server site name is generically referred to as www.sitename.com. The client/user 402 would typically enter this URL in their browser to contact the web site. A URL such as this can also have certain parameters associated at the end of the string (i.e. /home or /site). The presence of such parameters usually indicates that a client/user has
15 contacted (and/or bookmarked) a site previously, as these parameters typically provide a connection path which goes beyond the generic home page offered by entering only the site name. A lack of parameters might indicate that the client/user needs to be recognized. In this instance, the page request 404 is shown having no parameters. The merchant server 406 can be configured to cue on this lack of parameters, as a trigger for providing the various re-
20 directions described below.

For security reasons, a packet being exchanged between machines can be encrypted in such a way that the data is only valid for a short time. Hence, if somebody bookmarks a URL string, and then another unauthorized user pulls up that bookmark and tries to use it, the access will be valid for a limited time. Similarly, if somebody intercepts and/or copies the parameter
25 string, its use will be time limited. Hence, one solution offered by present invention is to treat the timed-out set of parameters as if the URL string has no parameters.

The merchant server 406 might similarly cue on other factors, but in this case the lack of parameters on the URL string serves as a convenient working example. The merchant server 406 would include merchant-side software, or the like, for detecting and acting upon whatever
30 factors are so used. One convenient method would include shipping a DLL to the merchant to

be included on their server device. A dynamic link library (DLL) is a collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file). When a DLL file is needed, it is then loaded and executed. DLL files are dynamically
5 linked with the program that uses them during program execution rather than being compiled with the main program. A set of such files is analogous to a set of library routines. The DLL might include a JAVA "servlet" (or the like) that implements the merchant-side code and logic.

10 The merchant server 406 will have previously registered via link 410 with a central server (or MV-CS) 420. As described above for Figure 3, a merchant ID 412, or the like, will be returned to the merchant server 406 for convenient identification of merchant information that might be databased on the MV-CS 420.

Link 422 next shows the merchant server 406 re-directing the client/user 402 to the MV-
15 CS with certain parameters. These parameters might include the merchant ID (412) as earlier established and retrieved from the MV-CS 420. The client/user 402 is thereafter shown sending its own associated re-direction 424, with the merchant ID parameter, and with any existing MV-CS cookies. If such cookies do not exist, then the client/user might be directed to register (or log-in) with the MV-CS 420. It should be noted that the re-direction is
20 accomplished by using an HTML "303" error, which is typically used to re-direct a user back to a known site if a requested page cannot be located and/or accessed. The re-direction 424 now places the client/user in the MV-CS environment 420, but with recognizable information about the client/user via the MV-CS cookie files, and with recognizable information about the merchant via the merchant ID.

25 The next series of re-directions involves the MV-CS 420 re-directing the client/user back to the merchant server with a certain identifying or return parameter which might be unique to that user (i.e. the user's name "John Doe"). Links 426 and 428 are shown directing the client/user 402 back to the merchant server 406 with this return parameter. The merchant server 406 can thereafter answer the original page request 404 by supplying the page 430.

30 This page 430 might include the original page information requested, but with a greeting like

"Welcome John Doe" at the top of the page -- as derived from the identifying or return parameter information.

Hence, the user will type an address such as `www.sitename.com` into the URL address line of the browser device. After the re-directions occur, the URL address line might resemble the following: `www.sitename.com/(username)?ccid=(control data coding)`. The re-directed parameters can be configured to return all the necessary information in one packet that could be interpreted by the recipient server. Alternatively, the parameter might provide an ID, wherein various server-to-server technologies might be used to communicate with the MV-CS database to retrieve the various pieces of information needed. Synchronization of a local merchant-side database and the associated MV-CS data could be performed on a periodic basis, however, the MV-CS centralized database is likely to contain the needed information. In the simplest case, a name (i.e. "John Doe") will be passed back in the parameter and used in a greeting on the page returned to the client/user. More complicated configurations would involve passing an ID back to the merchant server, wherein the merchant server would use this ID to extract information from a database (centralized or local) and build a specialized page with the requested information. Such would be the case for a web site that is not hosted on the MV-CS device 320. Alternatively, the MV-CS can actually host the merchant web site. The centralize database is thereby accessed directly (via a user ID or the like) as a function of the MV-CS being directly associated with the database.

If the user is unknown, then the returned parameter can be made to indicate such a condition. The necessary cookie files on the user's machine might not exist. They also may have been cleared, invalidated, timed out, or the like. The parameter can include the message "user unknown" or "user signed out". The page presented to the user, would therefore key on this parameter message and present a greeting like "Welcome new user" and/or provide directions for the user to sign in (via a "sign-in" link provided on the page, or otherwise). Referring now to Figure 4B, similar elements to those found in Figure 4A are shown. The merchant server 406 performs a registration 410 with the MV-CS 420 and receives a merchant ID 412. A page request 404 is sent from the client/user 402 to the merchant server 406. The merchant server 406 provides a re-direction 422 back to the MV-CS with certain (merchant) parameters. In this instance, the client/user is not known to the MV-CS 420, and hence the re-direction 427 will not contain any cookie information about this client/user. The subsequent

re-direction 429 and 431, from the MV-CS to the merchant server, will contain an indication in the parameter that this client/user is "unknown." The merchant-side software (e.g. DLL) will then re-direct 433 the client/user 402 to register 435 with the MV-CS 420. The cookie information (or file) will thereafter be set via 437 in the client/user device 402.

5 When the client/user 402 originally requested the page information from the merchant server, such a greeting could not have been provided. However, with the various re-directions described above, the client/user 402 can be greeted in a familiar way. The re-directions are virtually invisible to the client/user 402. If the merchant server 406 and the client/user 402 have each previously registered with the MV-CS 420, then the client/user can contact the
10 merchant server 406 for the first time, and yet still receive an individualized greeting. This described "greeting" is meant to serve as an example only. The parameter returned in link 428 might contain other types of information that can be used by the merchant server in fulfilling the client/user's page request.

 Referring now to Figure 5, a flowchart 500 is shown of certain representative steps that
15 might be used to set and utilize the cookie information for a particular client/user. Given that the present invention encompasses a multi-vendor system, two example web sites are shown contacting the central server (or MV-CS site). A first web site, referred to as www.AAA.com 502, is shown as an MV-CS enabled web site 504. Step 506 shows the user clicking on an e-commerce operation, such as an add-to-cart button. Given that this site is MV-CS enabled, the
20 AAA merchant ID 508 (or the like) will be passed with a service request directed to the MV-CS site 520. A second web site, referred to as www.BBB.com 510, is shown as MV-CS enabled 512. Step 514 shows the user clicking on the add-to-cart button, which similarly sends the BBB merchant ID 516 with a service request to the MV-CS site 520.

 Any MV-CS cookies that might exist will be passed onto the MV-CS site 520 with any
25 requests sent from the merchant servers or domains AAA (502) or BBB (510). Decision step 522 asks whether a cookie has been set. In other words, the configuration inquires whether any MV-CS cookies have been sent with the user request. If a cookie has been sent (e.g. "yes"), then it can be determined from the cookie the identity of the shopper making the request. Additional parameters that are passed along with the request, including for instance
30 merchant ID, sku, price, etc., can be used to further retrieve merchant information 540 from an appropriate database (or data store). There should now be enough information to add the user

selected item to the electronic shopping cart. The user can also be presented with a customized image of the shopping cart, as per step 530. The merchant ID can be used to access a database, which provides details regarding how this particular cart should look. The contents of the cart can be determined via the shopper ID, as derived from the incoming cookie information (e.g. from the user machine contacting the MV-CS site). As stated above, the add-to-cart operation is a representative example, and other operations might also be performed according to similar data flows.

Referring again to step 522, the cookie might not be set for a variety of reasons. The user might never have registered with the MV-CS machine, or may have switched user machines. In either case, no cookies would be available for passing with the MV-CS request. The user might also have signed off from an earlier session, which can (purposefully or otherwise) cause the cookie to clear, for security reasons and the like. Cookies might also be made to time out and clear after a set period of time (and/or inactivity). If the cookie is not set, then a sign-in screen 524 is presented to the user.

Decision step 526 queries whether the shopper has an account with the MV-CS system. If not, then the shopper is routed to appropriate forms (or the like) which allow the shopper to create an account, as shown in step 528. If the shopper has an account, then a sign-in (or log-in) option 532 is presented to the user. Upon completion of either step 528 or 532, the user information is available for setting the cookie 534 on the user machine that is associated with the MV-CS server. Once the cookie is set, then the user can be directed (as similarly described above) to step 530, wherein items are added to the shopping cart (or page) which has been customized according to the user and merchant information. The various pages are served back to the user to reflect a customized version of those pages.

The actual process of setting the cookie results in a page construction that contains appropriate coding to set the cookie information. One problem inherent to HTML browsers is that because the various re-directions are actually HTML "303" errors, such a process cannot be used to both set a cookie and re-direct the page in the same action. Because an error actually comes back, there is no HTML associated with the error, and hence no cookie information. Hence, the various re-directions must be configured to end up on a valid page, wherein HTML code will be present and a cookie (or cookies) can be set on the user's machine.

Referring now to Figure 6, a flow chart 600 is shown of certain representative steps that might used to facilitate setting the cookie in light of the various re-directions being performed. In general, the sign-in step sends a request for a sign-in page 602. The sign-in page sends a request to the MV-CS server 604, which validates the user by querying a database. Decision step 606 inquires whether there were problems validating the user. If yes, then the user is routed back to an information "fill-in" page 608. If there were no problems validating the user, then a server-side variable relating to "login successful" (or the like) is set. The user is next re-directed to a sign-in completion page, as shown in step 610. Upon completion, a server-side variable relating to "login done" (or the like) is set. Decision step 612 inquires whether this server-side variable has been set (or is present). If no, then the process is directed back to the fill-in page 608 (or the like) to gather the appropriate user information. If the server-side variable has been set, then step 620 shows the process returning an HTML page to the user's browser, with the HTML containing code for setting the cookie. Cookie setting code might exist as metatext, or HTML header code, or the like. Accordingly, the sign-in completion page (or its equivalent) allows the HTML (and cookie setting) code to be returned to the client device, wherein this could not be readily accomplished during a re-direction (or HTML "303" error) step.

While cookie information and cookies files have been described herein, the invention is not intended to be limited to such Internet specific examples. Any such client-side identity or information storage capability might similarly use the principles described in the present invention.

FIGS. 7A and 7B illustrate a generalized computer system 700 suitable for implementing various embodiments of the present invention. FIG. 7A shows one possible physical form of the computer system. Of course, the computer system may have many physical forms ranging from an integrated circuit, a printed circuit board and a small handheld device up to a huge super computer. Computer system 700 includes a monitor 702, a display 704, a housing 706, a disk drive 708, a keyboard 710 and a mouse 712. Disk 714 is a computer-readable medium used to transfer data to and from computer system 700.

The MV-CS described above, might be implemented on (or in association with) such a generalized device, like the one shown here. The MV-CS might also incorporate certain specialized features as described in U.S. provisional patent application No. 60/141905, entitled

"Multi-Vendor Internet Commerce System For E-Commerce Applications And Methods Therefor," Attorney Docket No. CCTYP001P, filed on June 30, 1999, and which has been incorporated herein by reference (above).

FIG. 7B is an example of a block diagram for computer system 700. Attached to system bus 720 are a wide variety of subsystems. Processor(s) 722 (also referred to as central processing units, or CPUs) are coupled to storage devices including memory 724. Memory 724 includes random access memory (RAM) and read-only memory (ROM). As is well known in the art, ROM acts to transfer data and instructions uni-directionally to the CPU and RAM is used typically to transfer data and instructions in a bi-directional manner. Both of these types of memories may include any suitable of the computer-readable media described below. A fixed disk 726 is also coupled bi-directionally to CPU 722; it provides additional data storage capacity and may also include any of the computer-readable media described below. Fixed disk 726 may be used to store programs, data and the like and is typically a secondary storage medium (such as a hard disk) that is slower than primary storage. It will be appreciated that the information retained within fixed disk 726, may, in appropriate cases, be incorporated in standard fashion as virtual memory in memory 724. Removable disk 714 may take the form of any of the computer-readable media described below.

CPU 722 is also coupled to a variety of input/output devices such as display 704, keyboard 710, mouse 712 and speakers 730. In general, an input/output device may be any of: video displays, track balls, mice, keyboards, microphones, touch-sensitive displays, transducer card readers, magnetic or paper tape readers, tablets, styluses, voice or handwriting recognizers, biometrics readers, or other computers. CPU 722 optionally may be coupled to another computer or telecommunications network using network interface 740. With such a network interface, it is contemplated that the CPU might receive information from the network, or might output information to the network in the course of performing the above-described method steps. Furthermore, method embodiments of the present invention may execute solely upon CPU 722 or may execute over a network such as the Internet in conjunction with a remote CPU that shares a portion of the processing.

In addition, embodiments of the present invention further relate to computer storage products with a computer-readable medium that have computer code thereon for performing various computer-implemented operations. The media and computer code may be those

5 specially designed and constructed for the purposes of the present invention, or they may be of the kind well known and available to those having skill in the computer software arts.

Examples of computer-readable media include, but are not limited to: magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROMs and holographic devices; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and execute program code, such as application-specific integrated circuits (ASICs), programmable logic devices (PLDs) and ROM and RAM devices. Examples of computer code include machine code, such as produced by a compiler, and files containing higher level code that are executed by a computer using an interpreter.

10 Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, any computer might act as a server, database, and the like, if properly configured. Therefore, the described embodiments should be taken as illustrative and not restrictive, and the invention should not be limited to the
15 details given herein but should be defined by the following claims and their full scope of equivalents.

CLAIMS

What is claimed is:

1. A networking method providing for sharing of cookie information between different web servers, the network including a central server device in network communication with at least one merchant server device, the devices in network communication with at least one client device, the method comprising:

registering at least one merchant server device with the central server device and providing merchant information, whereby an merchant identifier token is supplied to the merchant server device;

10 sending a page request from a client device to a merchant server device;

returning the requested page with an option to request an operation;

directing the operation request to the central server device along with the merchant identifier token, whereby available cookie information is passed from the client device to the central server device with the operation request;

15 retrieving the merchant information from the central service device via the merchant identifier token;

retrieving client information from the cookie information;

providing customized pages from the central server device to the client device based upon the merchant information and the client information.

20 2. The networking method of Claim 1, including the additional step of:

directing the client device back to the merchant server device upon completion of the requested operation.

3. The networking method of Claim 1, including the additional step of:

registering the client device with the central server device if the cookie information is not available, and setting the cookie in the client device.

5 4. The networking method of Claim 3, whereby if the registration process involves re-direction of a page, the cookie will be set via return from an HTML page that contains cookie setting code.

10 5. The networking method of Claim 1, wherein the operation includes an e-commerce related task.

6. The networking method of Claim 1, wherein the cookie information includes at least one cookie file or string stored on the client device.

15 7. The networking method of Claim 1, wherein the merchant information includes interface presentation style elements.

8. The networking method of Claim 7, wherein the merchant information is stored in a database associated with the central server.

20

9. A networking method providing for sharing of cookie information between different web servers, the network including a central server device in network communication with at least one merchant server device, the devices in network communication with at least one client device, the method comprising:

registering at least one merchant server device with the central server device and providing merchant information, whereby a merchant identifier token is supplied to the merchant server device;

sending a page request to the merchant server device with a triggering event;

5 using the triggering event to re-direct the page request from the client device to the central server with merchant parameter information, whereby available cookie information is passed from the client device to the central server device;

using the merchant parameter information and the cookie information to derive return parameter information;

10 re-directing the client device back to the merchant server device with the return parameter information; and

providing the requested page from the merchant server device to the client device, the page being customized based upon the return parameter information.

15 10. The networking method of Claim 9, further including the step:

registering the client device with the central server device if the cookie information is not available, and setting the cookie.

20 11. The networking method of Claim 10, whereby if the registration process involves re-direction of a page, the cookie will be set via return from an HTML page that contains cookie setting code.

12. The networking method of Claim 9, wherein the cookie information includes at least one cookie file or string stored on the client device.

25

13. The networking method of Claim 9, wherein the merchant information includes interface presentation style elements.

14. The networking method of Claim 13, wherein the merchant information is
5 stored in a database associated with the central server.

15. The networking method of Claim 9, wherein the return parameter includes an all inclusive string of information.

10 16. The networking method of Claim 9, wherein the return parameter includes an identifier to stored information.

17. A system architecture to facilitate the sharing of cookie information between different web servers, the architecture comprising:

15 a central server, with an associated database;

at least one merchant server device in network communication with the central server, whereby the merchant server registers with the central server device, with merchant information being databased according to a merchant index;

20 at least one client device in network communication with the merchant server device and the central server, whereby the client device registers with the central server device;

merchant server device software which recognizes a triggering event in a page request from the client device to the merchant server device,

25 whereby the triggering event causes the merchant server device to re-direct the page request to the central server device with the merchant index, the re-direction from the client device to the central server device transferring client device cookie information, the central

server device thereafter re-directing the client device back to the merchant server device with return parameter information.

18. The system architecture of Claim 17, wherein the requested page information is returned from the merchant server device to the client device, the page being customized according to information derived from the return parameter information.

19. The system architecture of Claim 17, wherein the merchant server device software is supplied to the server as a DLL.

20. A system architecture to facilitate the sharing of cookie information between different web servers, the architecture comprising:

a central server, with an associated database;

at least one merchant server device in network communication with the central server, whereby the merchant server registers with the central server device, with merchant information being databased according to a merchant index;

at least one client device in network communication with the merchant server device and the central server, whereby the client device registers with the central server device;

an operation selection option on a merchant server page,

whereby selection of the operation directs the client device to the central server device with the merchant index and available cookies being transferred therewith, the client device thereafter interacting with the central server to receive pages customized according to merchant information retrieved via the merchant index and client information derived from the cookie file information.

1/7

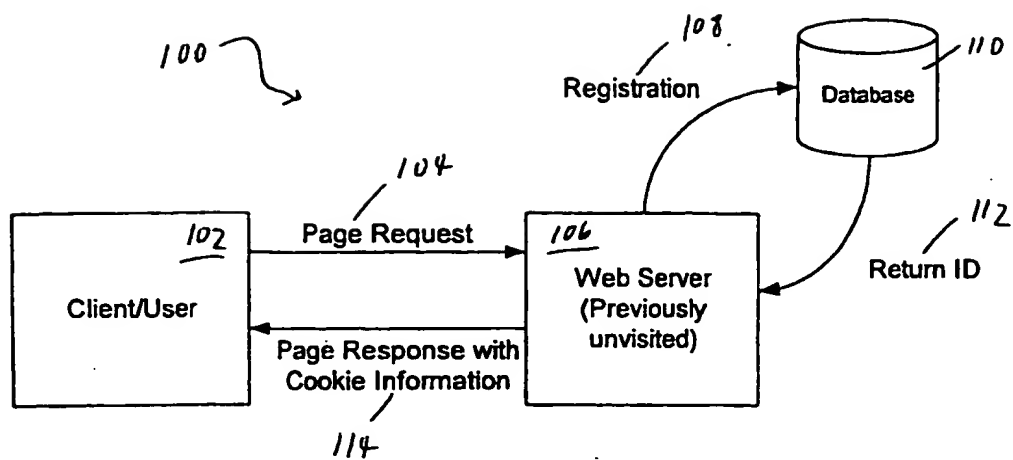


Figure 1 (Prior Art)

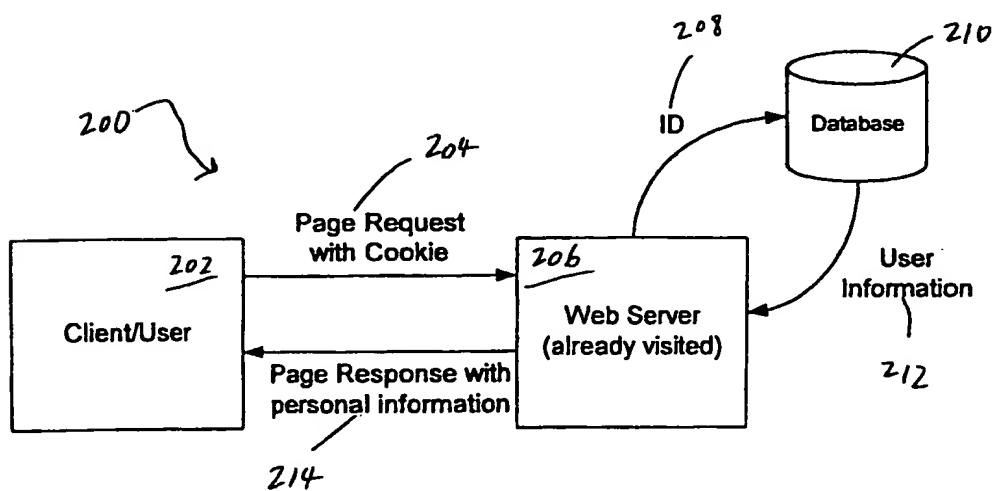


Figure 2 (Prior Art)

2/7

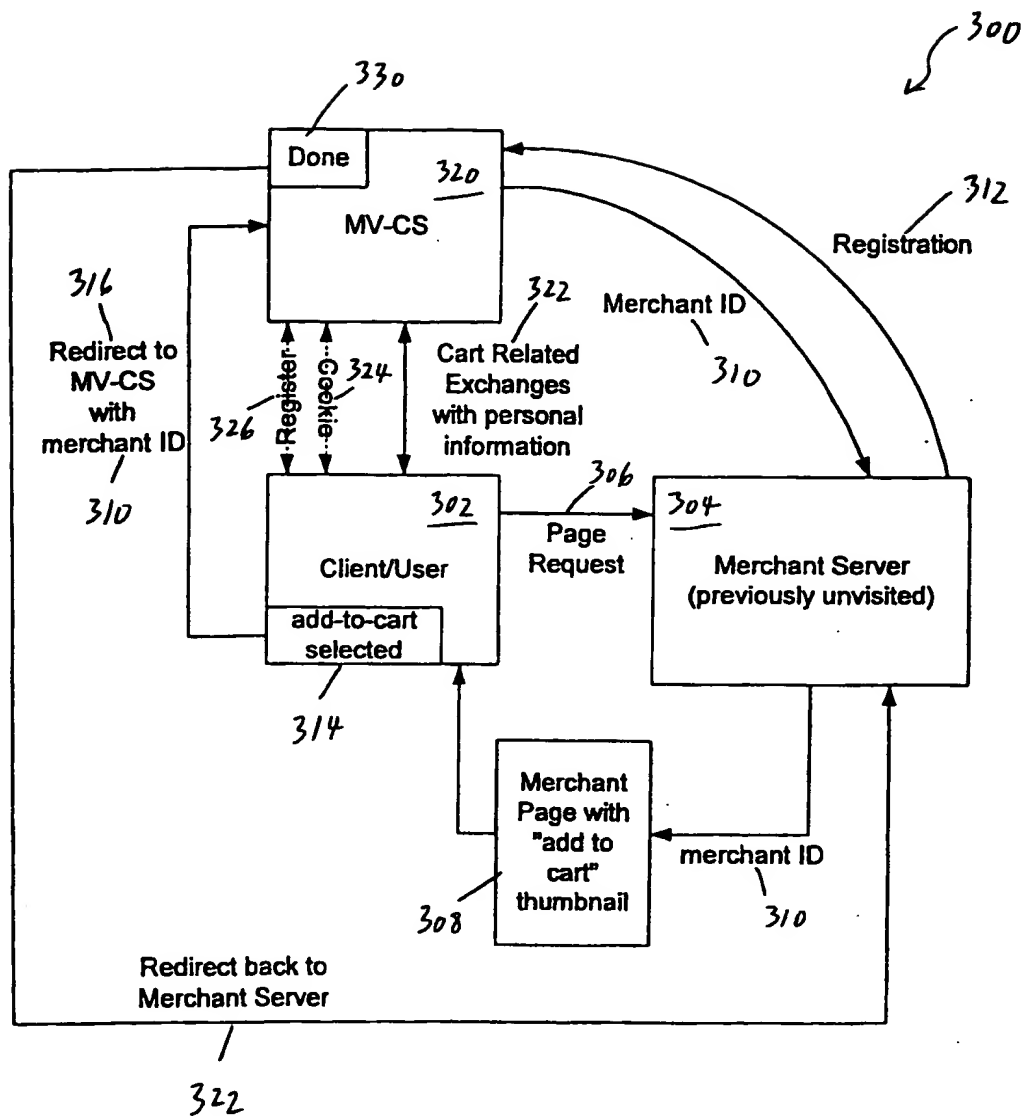


Figure 3

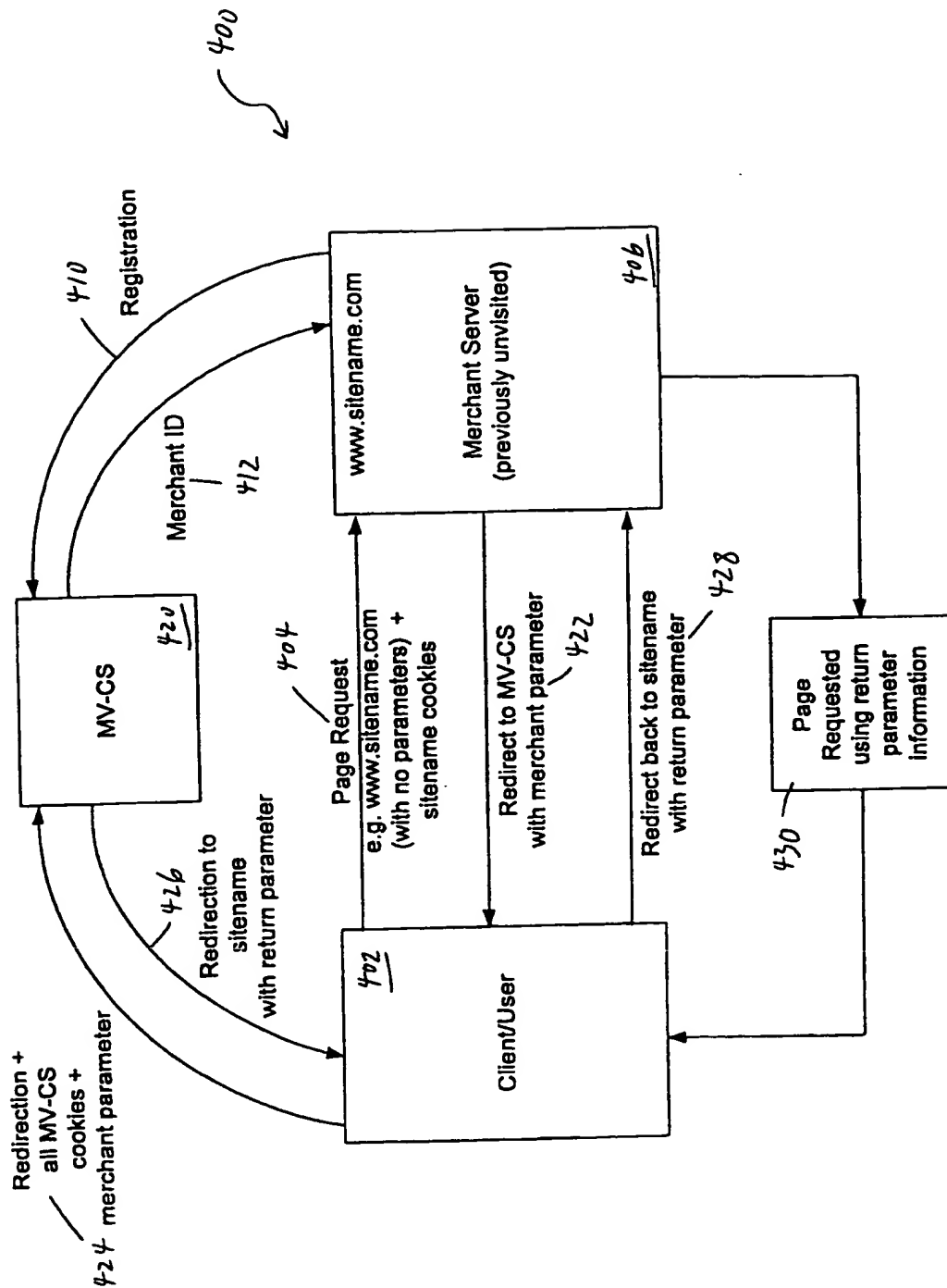


Figure 4A

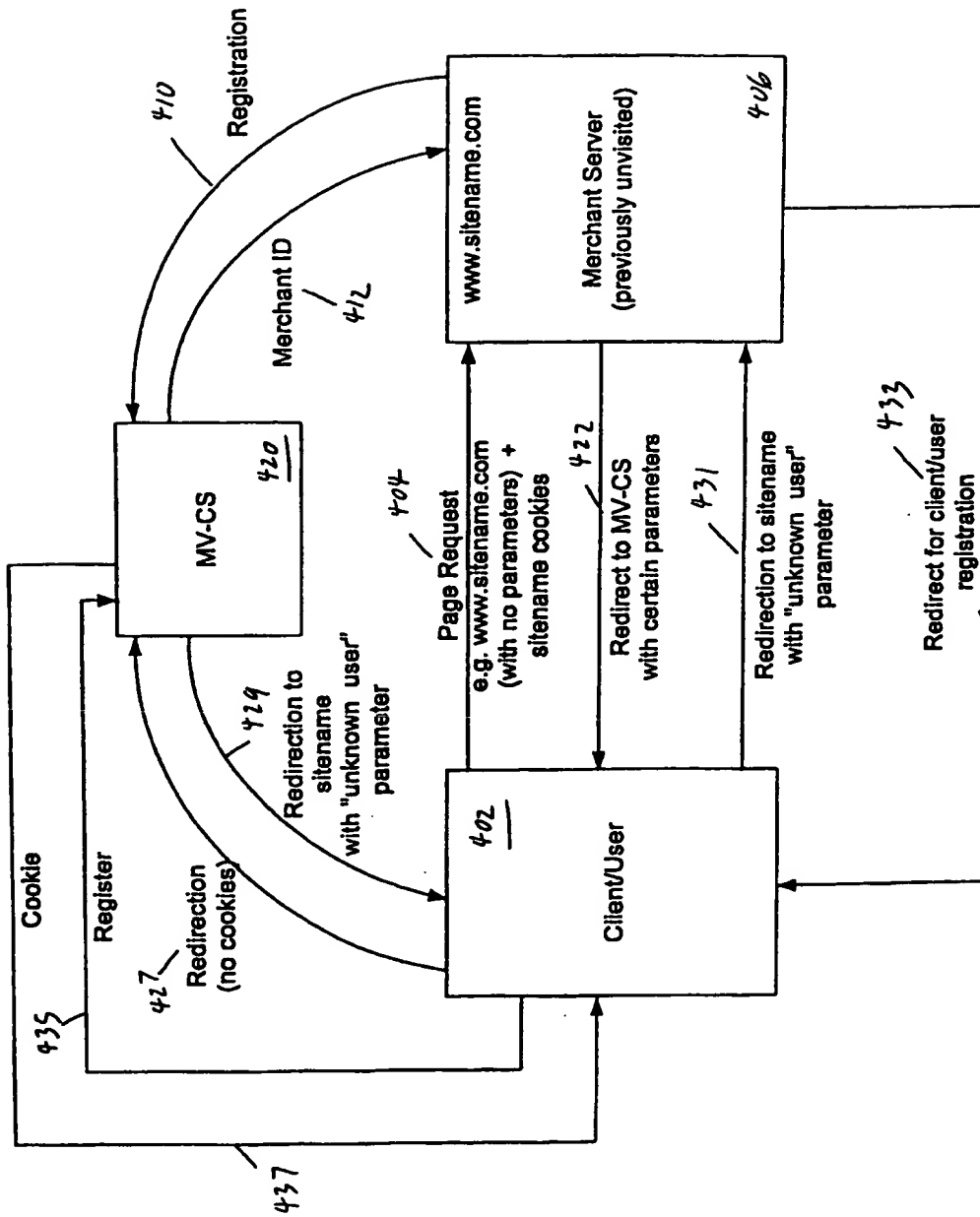


Figure 4B

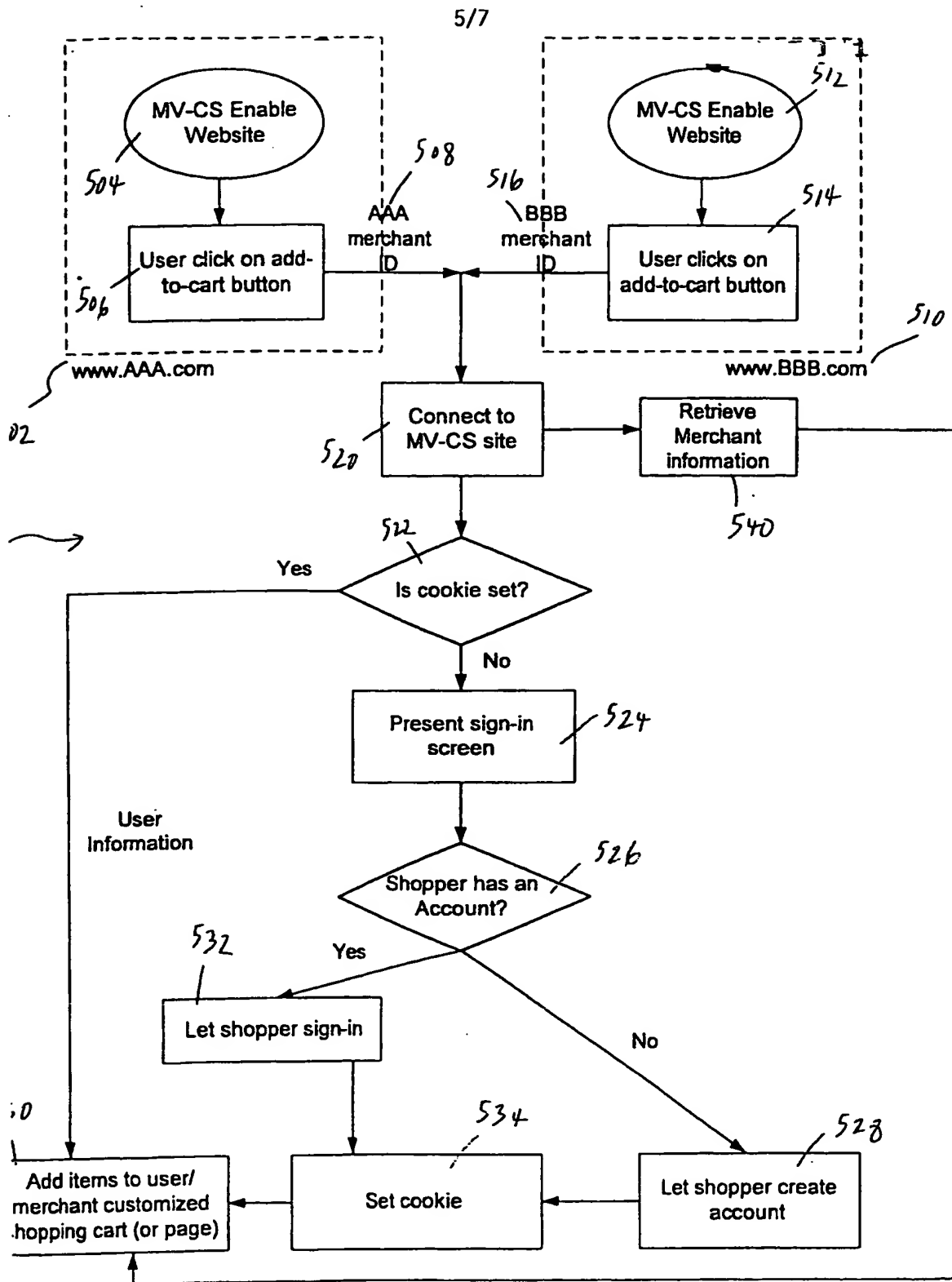


Figure 5

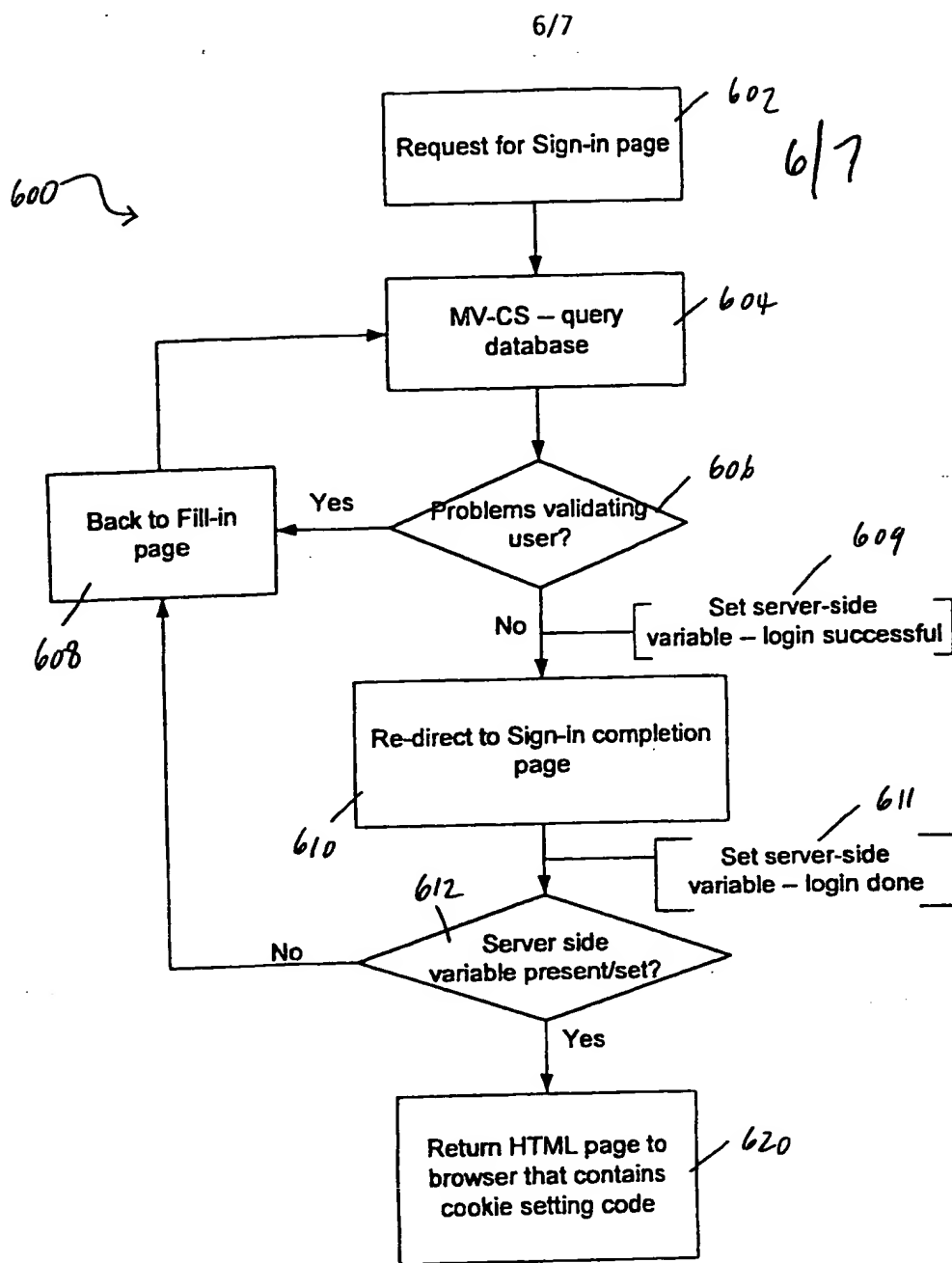


Figure 6

7/7

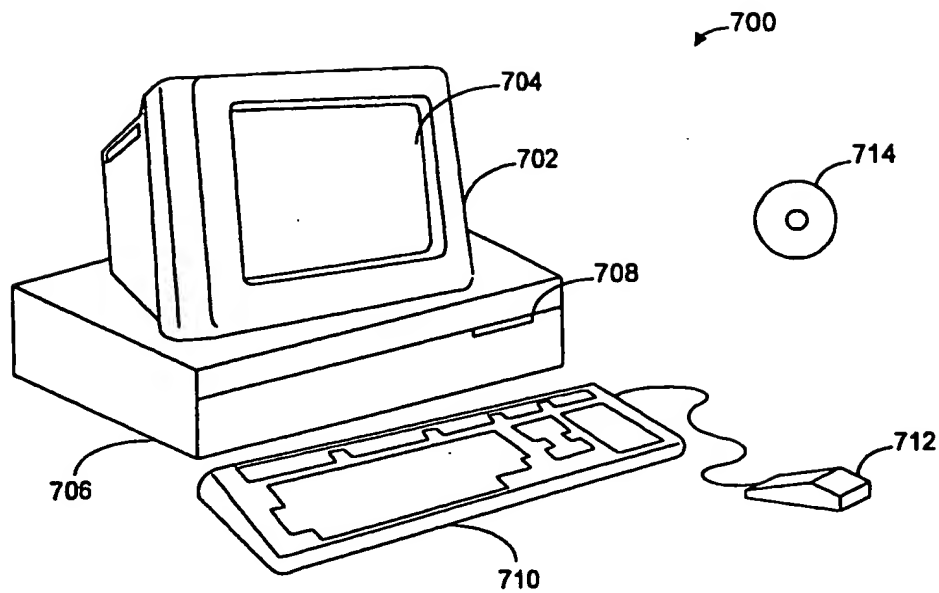


Figure 7A

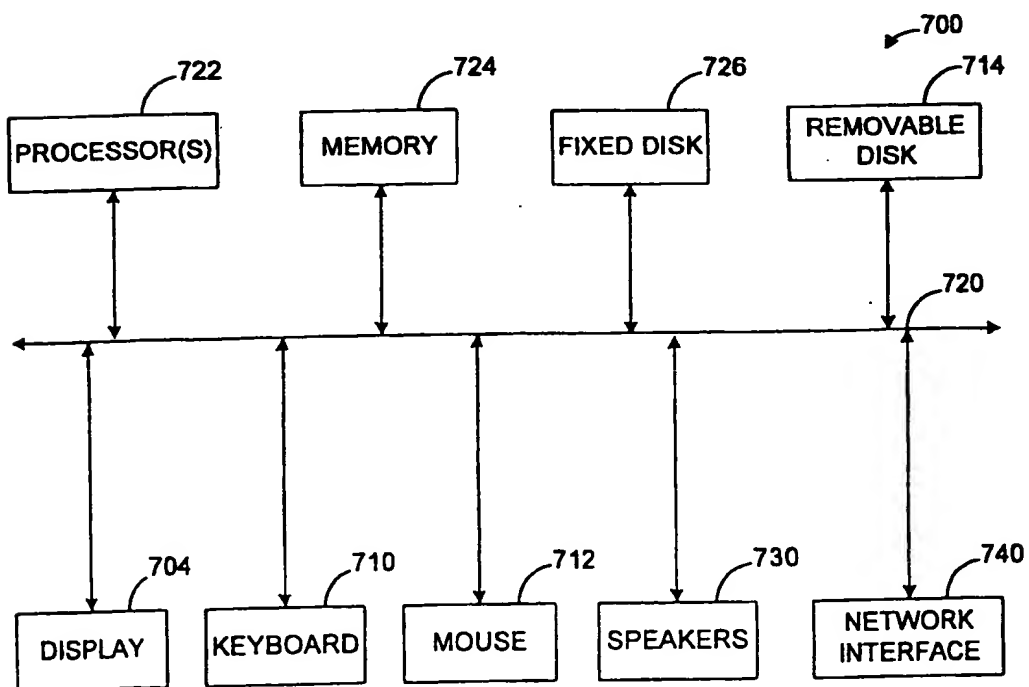


Figure 7B